

SmartPath Enterprise Wireless

The next generation of wireless technology—today.

- » Get fast 802.11n wireless.
- » Features smart controller-less architecture.
- » Intelligent APs automatically adjust for traffic, interference, and power conditions.
- » Ultra-reliable with no single point of failure.
- » Cloud-based management eliminates CAPEX.
- » Provides quality voice or video over Wi-Fi.



Indoors



Hardened/Industrial



Outdoors

SmartPath Enterprise Wireless System

The smart way to create an 802.11n network or upgrade an older WLAN or wired LAN for 802.11n Wi-Fi communications.

Black Box's SmartPath Enterprise Wireless system combines the stability, security, and speed of a wired network with the versatility and adaptability of a wireless network. It's just what you need to set up fast, 802.11n standard Wi-Fi communications in a logical way.

The technology differs greatly from existing wireless technology available today. You get speed and reliable wireless communications from a system that's simpler—and more affordable—to deploy.

With SmartPath, you get enterprise-class access points (APs) and a suite of management and security functions that provide all of the benefits of a controller-based wireless LAN (WLAN) solution—without requiring a controller or an overlay network.

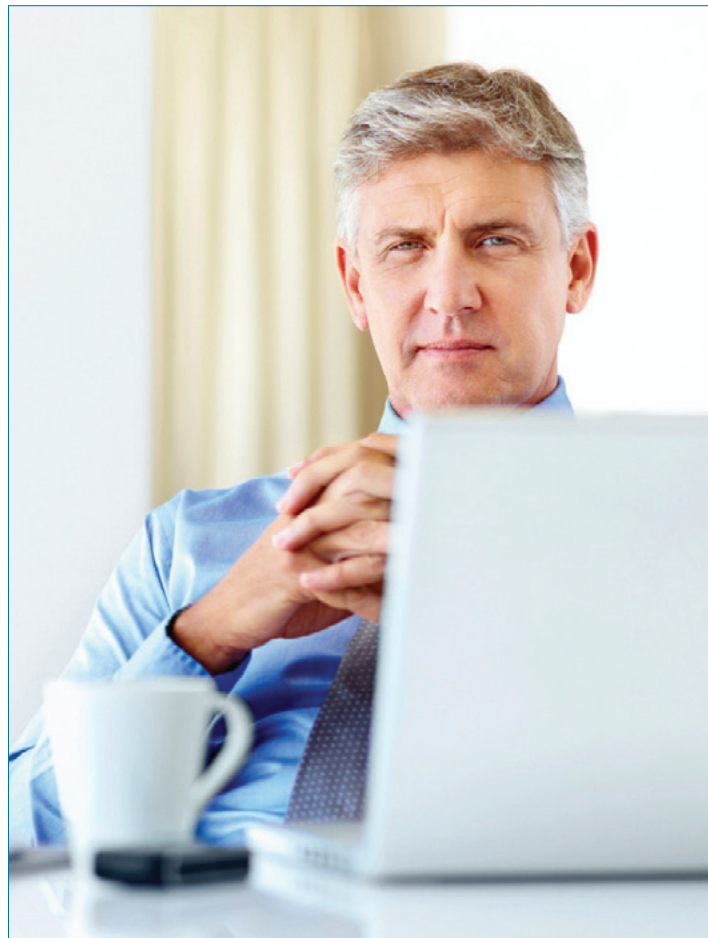
SmartPath APs work together to improve throughput and provide redundancy for your latest 802.11n wireless devices. The SmartPath system combines a distributed WLAN architecture and best-in-class management without a lot of upfront costs or operating expenses.

Black Box's SmartPath Enterprise Wireless system combines the stability, security, and speed of a wired network with the versatility and adaptability of a wireless network.

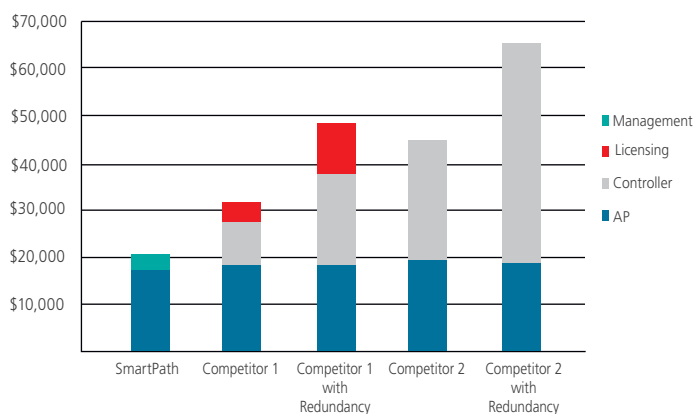
Because there are no expensive controllers required, you can expand from a few APs to thousands of APs easily—with no hidden upgrade costs. Start small, adding APs into an existing wired network as your budget allows, or build a complete enterprise-grade WLAN all at once.

Plus, the system boasts robust security and policy enforcement, including firewall and NAC functionality. Built-in RADIUS server and LDAP/Active Directory™ integration—along with a full-featured guest management system and portal—complete the system, making it perfect for organizations of all sizes.

- Reliability, throughput rivals that of wired networks.
- Supports video and VoIP communications.
- No expensive controllers needed.
- Smart APs sort and send packets to WLAN or wired points.
- Architecture reduces traffic backhauling. QoS and policy enforced right at the edge.



Cost comparison: SmartPath vs. top competitors*:



The best thing about SmartPath Enterprise Wireless is its performance. But don't ignore its very low cost of entry. Versus its two leading industry competitors, it's very cost effective with no big investment to start and no waste as you grow. The main reason: SmartPath's unique architecture eliminates the need for an expensive controller. Plus, you can manage it from the cloud (or a local appliance). If management is lost, the APs will function normally—no backup controllers are needed for redundancy!

* (30) Indoor SmartPath APs (LWN602AE) managed via the cloud using (30) SmartPath Enterprise Management System 1-Year Subscriptions (LWN600CM-1) vs. competitor systems with (30) APs, management software, additional licenses (if required), controller(s), and support costs.

NOTE: SmartPath Cloud-Based EMS Subscriptions are represented above as "Management" expenses, and there is no separate license purchase required.

The SmartPath architecture.

Unlike ordinary wireless systems, in which APs function as accessories to the wired network, SmartPath is designed as an *equal partner* to the wired network, making it a practical way to provide wireless across your organization.

First, SmartPath APs work much like the intelligent, smart switching devices found in today's wired networks, devices that actively sort packets and send them only to where they're needed—either to an attached node or to another switch or router for forwarding.

SmartPath APs sort and send the same way, broadcasting packets wirelessly, whether it's to a nearby Wi-Fi laptop user, passing them on to another access point in a wireless mesh arrangement, or sending them through the wired network to another endpoint.

It's really smart—and not something you'll likely find on today's average wireless APs, which function more like legacy network hubs and act only as interfaces to the wired network without making any decisions about where to send packets.

Plus, for seamless mobile user connectivity, SmartPath anticipates motion and proactively tracks users moving from AP to AP. This provides continuous coverage for voice or video applications without an interruption in service or having to connect and authenticate to each new AP. This is done automatically and is transparent to the end user.

Also, advanced circuitry and algorithms enable older 802.11a/b/g devices to share the network without slowing down 802.11n devices.

How SmartPath works.

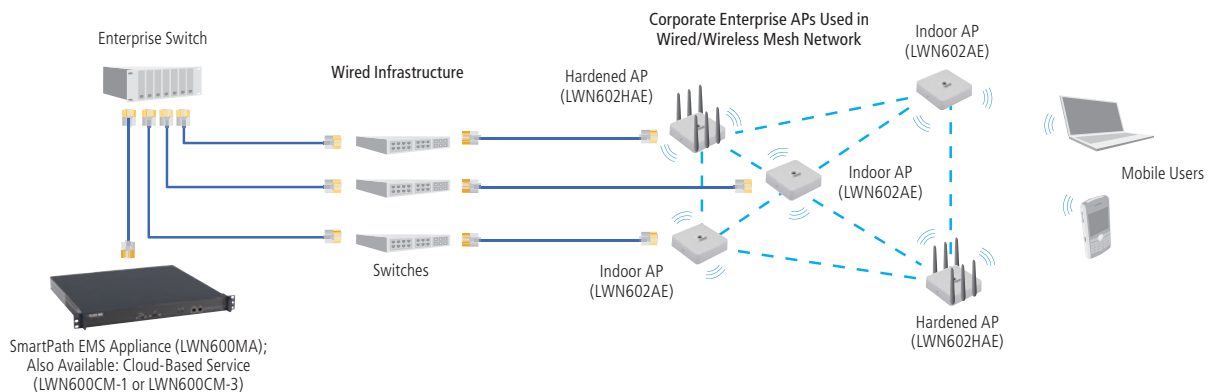
SmartPath uses a collaborative control design based on the same architectural premise behind dynamic routing protocols used by WANs and the Internet, and the Spanning Tree protocols of LANs: By distributing the control and data plane, redundancy and optimization are built into the system, and by centralizing management functions, the entire system can all be run from one location—even from the cloud.

This collaborative design enables multiple APs in the SmartPath network to be organized into groups, or clusters. These clusters of APs "talk" to one another, sharing control information and enabling fast Layer 2/Layer 3 roaming and seamless mobility for users, cooperative RF management, higher security, resiliency, and more.

SmartPath APs discover each other no matter if they're connected to each other over a wired network or linked wirelessly. When neighboring APs are found with the same cluster or mobility credentials, the APs build secure connections to each other. They then use special protocols to provide best-path data forwarding.

This way, APs can dynamically route around any problems or failures, and adding another site is as simple as adding another AP. You never need to upgrade to a higher-capacity controller when you have to add one or more APs.

What's more, the SmartPath network architecture is more reliable and higher performing—and more suitable for voice-over-wireless LAN—than most controller-based architectures.



- » Optimized for real-time traffic, 720p video, and VoIP—great for voice over wireless LAN (VoWLAN).
- » Advanced controller-less architecture improves network performance and saves you money.
- » Incorporates legacy 802.11a/b/g wireless devices with no degradation in 802.11n performance.
- » APs work together to improve speed and redundancy.
- » APs are easy to manage from the cloud- or appliance-based SmartPath Enterprise Management System.
- » APs work as intelligent, self-aware devices within a distributed, self-healing mesh network.
- » Scalable from one AP all the way up to a wide-area wireless network with thousands of APs.
- » Supports Gigabit Ethernet links to a wired network.
- » Secure with access enforced by per-user policies and SLAs.
- » Uses advanced WIDS and wireless VPN communications for secure, seamless roaming.
- » PoE-powered APs for reduced power infrastructure needs.
- » Resilient. No bottlenecks, no single points of failure.
- » Uses collaborative APs instead of controllers.
- » Enables secure, fast Layer 2/Layer 3 (L2/L3) roaming.
- » Standard or hardened AP models available.

SmartPath Wireless: Applications

It's the ideal wireless upgrade solution for:

K–12 schools.

SmartPath is a perfect match for K–12 institutions because it's affordable and easy to set up and use—which makes it attractive to busy school IT staff. It's great for district-wide wireless deployment, with the ultimate goal of having Wi-Fi coverage in every building.

But it also enables administrators to meet security requirements when deploying WLANs, particularly when it comes to maintaining CIPA compliance. SmartPath gives you the ability to set up multiple VLANs within one wireless network so you can simultaneously lock down student PC access while allowing staff the freedom to browse the Internet. You can set up guest VLAN access as well.

Segmenting a school's WLAN is possible because the system enables administrators to assign different SSIDs and restrict IP ranges by individual users or groups of users.

Plus, there are none of the drawbacks of having a network controller that supports a fixed number of APs—that is, when you've reached your AP limit, you're not forced to buy another controller along with all of its associated licensing fees. With SmartPath, the intelligence of the controllers is embedded in the APs themselves. There is no steep upgrade path. When it's time to expand, just plug in extra APs.

Because it supports the latest 802.11n devices, staff members can use iPad®, iPhone®, or other mobile devices to access information whenever they're within range. Having devices on Wi-Fi rather than a cabled network makes teachers' jobs easier and maximizes classroom time.



- » Better network performance. No controller bottlenecks.
- » Reduce CAPEX in your IT budget. "Pay as you grow."
- » Easily handle dozens of simultaneous users with each AP or thousands of users with several APs.
- » Helps you comply with school Web security mandates.
- » Use to track school laptops and other tagged assets.
- » Simple to separate staff equipment from student devices.
- » QoS and SLA functionality is built in.

Higher learning.

SmartPath is great for universities, colleges, trade schools, and other higher-education institutions, especially those who need to give students campus-wide wireless access but are finding it difficult to do as they experience funding shortfalls.

With 802.11n support, SmartPath gives schools higher throughput and more channel availability to a myriad of newer wireless devices (laptops, smartphones, tablets, and others). Even better, SmartPath is robust enough to support traffic-intensive campuses with hundreds or thousands of concurrent users.

Plus, SmartPath can enhance a university's existing network access control (NAC) efforts where you need to segment users by different groups. Each group has its own security policies.

SmartPath fits well into large, campus-wide infrastructures without adding maintenance and management complexity for your limited staff. You can install the system components in classes and dorms over a weekend or on break. Hang the APs, plug them in, and walk away. Any management or configuration work can be done from a central point and pushed out to all APs simultaneously.

Without controllers to limit growth, SmartPath offers true scalability, enabling your IT staff to add APs one by one as needed. This architecture also reduces traffic going up through your network core, improving overall performance and eliminating single points of failure.



- » Controller-less design eases campus network upgrades.
- » Gives staff and students the 802.11n speed they desire.
- » Simplifies faculty access to network-shared applications.
- » Distributed architecture for resilient campus-wide links.
- » No sending traffic back to LAN controllers at the core.
- » Simple to update APs. Reconfigure all APs in seconds.
- » Easily provide network access for authenticated users and Internet-only access for other devices.

Enterprise.

If you're looking to upgrade your enterprise's wireless network to fill dead zones and support VoIP and video, as well as bring branch offices on-line inexpensively, then the SmartPath system is for you.

The distributed, easily scalable solution enables you to increase WLAN capacity without the need to spend a lot on a controller-based system. Plus, unlike "fat" APs, which can be quite cumbersome to manage and require manual maintenance, SmartPath APs feature software that enables them to self-organize into clusters and intelligently share network control information with one another.

You not only reduce the data bottlenecks and latency associated with the backhauling of traffic through controllers, you also create fault tolerance. Dynamic mesh failover enables traffic to be routed around failures in the wired network by dynamically establishing a wireless mesh connection among neighboring APs—great for mission-critical applications.

The result is an enterprise-class solution for management, mobility, and security at a more reasonable cost—from your central office to the edge of your network. Deploying an expensive controller for just a few access points in a satellite office simply doesn't make financial sense. Not when you can use SmartPath APs instead.

Plus, with SmartPath, you can support the amount of throughput required by video applications and smartphones while ensuring maximum uptime and enhanced quality of service (QoS) for multimedia and time-bounded voice traffic.



- » Optimum performance for each wireless traffic type, including latency-sensitive voice and video.
- » Supports mixed 802.11n and legacy 802.11a/b/g users. Slow clients won't impact performance of faster clients.
- » Offers a linear cost curve—no steep upgrading expense.
- » Eliminates controllers from the network. No need for an expensive controller in each branch office.
- » Provides fast, secure roaming and identity-based security.
- » The network "self heals" around any failure points.
- » Group policy settings for automatically creating wireless profiles for users, transferable from one office to another.
- » Easy to manage entire enterprise from a central site.

Retail and distribution.

Bringing local mobile Wi-Fi connectivity to companies that have multiple geographically distributed sites can be an overwhelming, and expensive, task. Not so with SmartPath. Central management features simplify the deployment and control of disparate wireless LANs in a distributed architecture.

And because there are no controllers involved, you can scale your operations by adding SmartPath APs one by one as your budget allows.

For retail, SmartPath gives you an easy, cable-free way to reach PoS/PoP terminals and stream video to in-aisle displays.

By design, the system has no single points of failure, so you can maintain real-time wireless connectivity in stores and warehouses even if one connection fails. A simple management interface enables you to deploy a wireless inventory control system site by site by pushing data from a central office to all newly installed APs.

SmartPath also offers secure roaming and identity-based security enforced at every AP, as well as over-the-air encryption. SmartPath also includes firewall, VPN, RADIUS, and Active Directory support. This way, you can lessen concerns over credit card privacy and better meet PCI DSS mandates.

Plus, with 802.11n support, you get better speed and performance. Drivers, warehouse workers, and other staff can use the latest handheld devices to scan, log, and perform other tasks while linking to bandwidth-intensive applications as they roam.



- » No need for a controller in each retail store or at a distribution point.
- » Great for companies with limited IT staff and budget.
- » Reduces operating expenses as well as downtime.
- » Less hardware required for each store or site.
- » Distributed architecture for failover routing of data.
- » Use a single GUI interface to set global policy management and centrally configure and monitor wireless connectivity.
- » Integrates with endpoint compliance systems.
- » Hardened options for use in factory or industrial settings.

SmartPath Wireless: Applications

Hospitals and healthcare.

Hospitals are trying to improve efficiencies and reduce costs, and as a result, IT is expected to do more with less. SmartPath makes it happen. It enables you to more cost-effectively bring high-speed wireless networking to all areas of your facility. Simultaneously, you can better support core care while trimming IT equipment and operational expenses.

Because it supports higher speeds and 802.11n connectivity, SmartPath greatly assists the mobility of today's caregivers and the growing use of networked imaging and video in patient care. What's more, the distributed yet centrally manageable architecture can handle large amounts of traffic and provide fast data availability to clinicians.

SmartPath is great for deploying wireless across an entire health system with Wi-Fi coverage in every building—including seamless roaming. Nurses and physicians can have access to critical applications and information from patients' bedsides.

Segment access, too. Give visitors Internet access while allowing staff both Web and secure access to the private hospital network. Go further and create VLANs within a wireless network to allow only certain staff access to medical records. Allow patients to securely connect to the Internet without the fear of them getting into your network.

SmartPath's mesh technology enables direct AP-to-AP communications, so there's no need to cable to switches in ORs and other "clean areas." The mesh technology also works well in older hospitals with concrete walls, where other RF products fail.



- » Fast yet secure. Helps maintain compliance with the network security aspects of HIPAA privacy mandates.
- » Brings greater mobility to doctors and other caregivers.
- » Supports tracking of equipment with built-in 802.11n tags.
- » Fully distributed processing and data forwarding for ensuring maximum WLAN connectivity .
- » Reduce CAPEX for new hardware. No controller purchases required; incrementally add an AP as money allows.
- » IT staff can manage hospital WLAN from a single console.
- » Easily provide Internet access for patients.
- » Works well in challenging RF environments.

Also great for:

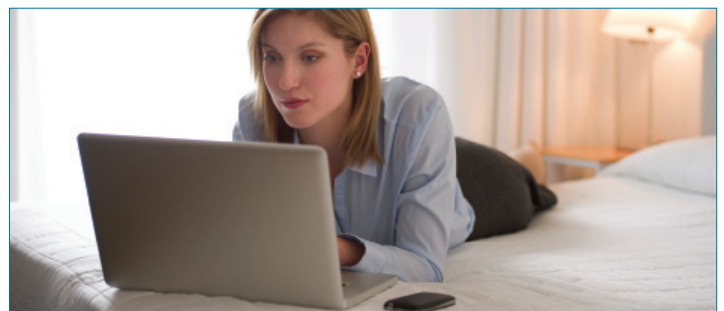
Government

- » What you need for mission-critical, fast 802.11n wireless in federal and state agencies with highly distributed organizational structures.
- » For offices with stringent security requirements, supports central enforcement of identity-based security and access control.
- » Ideal for departments with uncertain future funding. Leverage existing networks while migrating from controller-based, "thin" AP networks.
- » An economical way to bring Wi-Fi to local community centers, civic centers, libraries, transit facilities, courthouses, and city halls.



Hotels and meeting halls

- » Give guests fast, reliable Wi-Fi connectivity with seamless roaming.
- » Hotel chains can centrally manage multiple sites from the cloud.
- » No server or controller installation to worry about. Sets up easily without disrupting guests' stays.
- » Resilient, mesh architecture is ideal for maximum wireless network coverage at hotel resorts and large, multiroom convention centers.
- » Plug and play. Great for temporary setups by event organizers.



Growing small businesses

- » Autonomous APs allow for a low-cost deployment. Capacity can be added linearly when needed—no costly controller upgrades.
- » Supports the speed and bandwidth required of VoIP and video.
- » Easy to set up Internet access for visiting customers or vendors while separating them from your WLAN users.
- » Offers quick setup with browser-based SaaS management.



Get ready for the move to 802.11n standard Wi-Fi networks in the coming years.

Productivity



Mobility



Applications



Users

Yesterday's WLANs:

- » Wi-Fi for convenience
- » Nomadic users
- » Limited speed and range
- » Best for smaller office networks
- » An extension of the wired LAN

The 802.11n world:

- » Ideal for mobile users
- » 10x bandwidth potential
- » MIMO antennas for more range, better coverage
- » Dual-mode voice capable
- » Possible wired Ethernet replacement

The needs of enterprise Wi-Fi are growing.

The way that Wi-Fi is being used and the requirements on an enterprise Wi-Fi network are going through a fundamental and generational change. The reason: There's an explosion of Wi-Fi enabled devices, a 10x performance increase with the 802.11n standard, and the migration of Wi-Fi from convenience to mission-critical Ethernet networks.

As a result, the enterprise is demanding a new type of wireless LAN infrastructure. SmartPath technology is designed to meet that demand. With it, your enterprise can get a secure multiservice infrastructure that's capable of supporting voice, video, and data users—as though they each had their own networks. QoS and SLA features help ensure end-user experiences are maintained.

Enterprise users also want the mobility and productivity of Wi-Fi with the scale, performance, resilience, and ubiquity of the Internet. To that end, SmartPath enables you to create a widely accessible, low-cost, network with wire-like resilience that is also easy to deploy and use.

The network impact of 802.11n.

Centralized data forwarding is usually sufficient for 802.11a/b/g wireless networks, where network speeds were much lower. But as more bandwidth is used for 802.11n, this centralized approach has a huge impact on backbone links and the controller itself.

But without a controller, you can minimize such backhauling of data. SmartPath's architecture offers all the wireless functionality promised by 802.11n in a controller-less design, so:

- Data traffic flows from wireless clients to the AP, then to the client's destination in a direct, open path.
- Control traffic is localized and flows only between APs that are in the same RF neighborhood.
- No required "double-switching" tunneling or single points of failure. Traffic works just as it does on your wired network.
- Data traffic from higher-speed radios is distributed across the network, is not bottlenecked in to and out of a single device, and doesn't need to hit the core.
- Wireless traffic is no longer opaque to the rest of the network. Your WLAN benefits from security and QoS schemes already in place.
- Policy enforcement can be provided at network edge, instead of at the controller.

The standard model for indoor-only applications:

SmartPath Enterprise Wireless Indoor AP (with Integrated Antennas)

- » Once plugged in, automatically joins the network and contacts the system's SmartPath EMS software for configuration or security setting updates.
- » Integrated dual concurrent 2.4-GHz/5-GHz MIMO antennas.
- » Scalable from one AP up to thousands of APs.
- » Supports Gigabit links on a 10-/100-/1000-Mbps RJ-45 port.
- » Fits into most office decors. PVC exterior can be painted.
- » PoE powered device for reduced power infrastructure needs. External power supply also available.
- » Uses advanced WIDS and wireless VPN communications for secure, seamless roaming.
- » Supports legacy 802.11a/b/g and 802.11n devices, too.

The single-processor SmartPath Enterprise Wireless Indoor AP (with Integrated Antennas) uses two integrated radios to provide an aggregate link speed of 300 Mbps.

It's more sophisticated than today's average AP, which typically functions more like a network hub, acting only as an interface to the wired network without making decisions about where to send packets. The SmartPath AP, however, works like a high-end switch, sorting packets and sending them to where they're needed.

The SmartPath system can even track a user moving from one AP to another, providing the most efficient throughput. Advanced circuitry and algorithms allocate air time efficiently, enabling older 802.11a/b/g devices to share the network without slowing down 802.11n connectivity.

An enterprise-grade solution that's secure.

The SmartPath Enterprise Wireless Indoor AP contains the features you'd expect from an enterprise-grade wireless product, including Layer 2 switching, VPN tunnels, and QoS support.

Plus, it has robust security and policy enforcement, including NAC functionality and LDAP/Active Directory integration. Because the RADIUS is built in, there's no need to purchase and deploy a separate RADIUS for authenticating users or devices before they're granted access to your network. The AP also has onboard stateful-inspection firewall policy enforcement with session state sync with neighboring APs.

No bottlenecks or latency for bandwidth-heavy applications.

Because the SmartPath Enterprise Wireless Indoor AP functions as a self-aware, smart device without the need for controllers in your enterprise, you can eliminate the bandwidth bottlenecks and latency that result from backhauling traffic through a controller. This, in turn, enables you to create an ideal platform for demanding applications, such as voice over wireless LAN (VoWLAN) deployments.

For RF management, the AP offers cooperative channel selection, with DFS2 support, as well as client load balancing. It can also automatically increase airtime allocation to clients best able to use it.



LWN602AE

SmartPath includes SLA functionality, enabling the APs to monitor the connection quality and, if necessary, automatically trigger and report on actions to improve quality. Performance and connection quality are continuously compared to target service levels, and the SmartPath network automatically responds when service levels do not meet those targets.

Easy to set up, power, and manage.

The SmartPath Enterprise Wireless Indoor AP works as a PoE device, so you can power it through Ethernet wiring from a PoE injector or plug it into a nearby wall outlet (with the optional power supply kit). The AP intelligently uses whatever power is available at any given time, from any power source.

Once plugged in, each AP automatically joins the network and contacts the SmartPath Enterprise Management System (EMS). Available as a cloud-based service or a standalone appliance, the EMS is a versatile platform that enables you to manage all APs in your entire wireless network from a single, user-friendly GUI console. (For details on the EMS platform, see [page 10](#).)

If the APs lose communication with the SmartPath EMS, all AP functionality is preserved so there is no loss of uptime.

Fits well into the typical office environment.

The SmartPath Enterprise Wireless Indoor AP can be used in any standard office environment. Mount it on the wall with screws, or fasten to a ceiling with its tile clips (an optional drop ceiling bracket is also available). It is plenum rated.

Its off-white exterior blends inconspicuously into most office decors. A muted LED light radiates from beneath the Black Box logo on its top cover, gently glowing instead of blinking, emitting a specific color light to signal operation status to IT personnel without distracting others nearby.

And to protect it from theft, the AP can be used with Kensington® style locks and features a tamper-proof security screw.

For specifications and other features, see [page 11](#).

The hardened model for harsh indoor or sheltered outdoor applications:

SmartPath Enterprise Wireless Hardened AP (without Antennas)

- » All the features, range, roaming, and scalability of the standard AP but in a hardened design.
- » Use in harsh indoor industrial areas, or in a sheltered outdoor location (separately sold outdoor kit required).
- » Features dual-core processor and six RP-SMA connectors.
- » Pair it with separately sold antenna kit or outdoor kit containing antennas, a NEMA rated housing, hardware, and a lightning arrestor.
- » Once plugged in, automatically joins the network and contacts the system's SmartPath EMS (order separately).
- » Dual 10-/100-/1000-Mbps RJ-45 ports.
- » Smart PoE (802.3af/at) powered. Or use with optional standalone AC power supply.



LWN602HAE

The SmartPath Enterprise Wireless Hardened AP (without Antennas) features a dual-core processor and uses two radios to provide an aggregate link speed of 300 Mbps. It's much like the standard office version on [page 8](#) but is designed specifically for use in harsh areas.

Like the standard model, the hardened version works like a high-end switch, intelligently sorting packets and forwarding them as needed. Plus, like the non-hardened version, it works with other standard and hardened APs to create a self-aware, self-healing mesh network with no single points of failure.

The SmartPath Hardened AP, however, features external antenna connections, providing extra flexibility. You choose antennas separately depending on your application and RF needs.

Available antenna and outdoor mounting options.

If you order the SmartPath 602HA Antenna Kit (LWN600A-ANTK), you get six antennas that attach to the six RP-SMA connectors on the sides of the access point unit. These antennas suit **indoor** applications only.

We also include antennas in our SmartPath 602HA Outdoor Kit (LWN600A-OUT), but instead of six antennas, this kit has four dual-band omnidirectional antennas that plug into the N-Type connectors on the top of the outdoor kit's enclosure.

The outdoor kit includes everything you need to mount the access point, including a NEMA 4X and 6P (IEC IP56/IP67) rated enclosure assembly. For optimum radio transmission, the enclosure features an adjustable vertical orientation.

Offering protection from the elements and a temperature tolerance of 13 to +140° F (-25 to +60° C), the outdoor enclosure assembly can be mounted to a pole or on a flat surface. The included pole bracket fits a pipe with a 1" to 3.5" (2.5 cm to 8.9 cm) diameter.

In addition to an outdoor enclosure and mounting hardware, the outdoor kit includes a patch cable and a lightning arrestor device that offers electrical surge protection on the Ethernet line.

For specifications and other features, see [page 11](#).

WARNING: To install the access point and outdoor kit safely, you must be a qualified installation professional, licensed or certified in accordance with local regulations.



LWN600A-ANTK



LWN600A-OUT (shown with the LWN602HAE installed).

Also manageable via the cloud or EMS appliance.

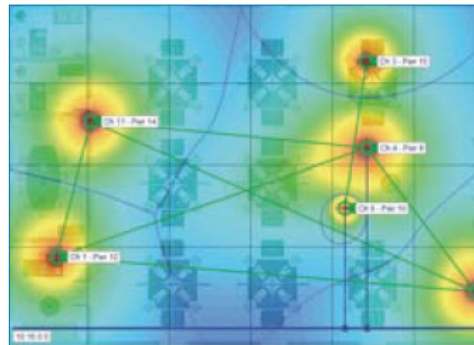
Like the standard APs, the hardened APs are managed through the separately purchased SmartPath Enterprise Management System (EMS), available as a cloud-based service or a standalone appliance. For details, see [page 10](#).

SmartPath Wireless: The Management Platform

For managing all APs and your network, order:

SmartPath Enterprise Management System (EMS)

- » Available as cloud-based subscription or standalone network appliance.
- » Manage entire system from a user-friendly GUI console. APs can be configured in minutes through the EMS.
- » Platform's policy-based management simplifies large deployments encompassing many sites and offices.
- » Use to set up access enforced by per-user policies and role-based guest management delegation with SLAs.
- » Group policies can be applied network wide to all APs or individually to certain APs.
- » Integrated Wi-Fi planner tool helps you verify optimum SmartPath Wireless AP placement.
- » Easily see network topology and status of access points.
- » Boasts full 802.1X authentication for secure access.
- » Supports RADIUS with Active Directory, LDAP, Open Directory, and eDirectory integration.
- » Easily manage security settings, firewall policies, and more.



The EMS interface includes a helpful Wi-Fi planning tool.



SmartPath EMS Appliance (LWN600MA) installed in a data center.

The SmartPath Enterprise Management System (EMS) brings best-in-class management to a distributed WLAN system comprising several or hundreds of SmartPath APs.

Once plugged in, each SmartPath AP automatically joins the network and contacts the EMS using the secure CAPWAP-DTLS protocol. Configuration data is then pushed from the EMS to the newly installed access points for true plug-and-play installation.

What's more, the SmartPath EMS provides centralized control without being actively involved in passing traffic or making forwarding decisions. This way, you get advanced administrative control without creating the traffic bottlenecks seen with some controller-based wireless solutions.

Provides complete SmartPath WLAN visualization.

This GUI platform enables you to manage the entire SmartPath system from a user-friendly GUI console. It features a customizable dashboard and gives you advanced functionality without unnecessary complexity. Use it to monitor, upgrade, troubleshoot, and more.

Network maps enable you to see topology and status of APs, and real-time heat maps show RF propagation within your enterprise. The EMS detects both authorized and rogue WLAN clients and access points, and places them on a map.

Screens also feature details related to SLA compliance and statistics for reporting purposes. Configuration audit capabilities ensure that all configurations are up to date, and you can set up real-time monitoring of alarms and events from all APs.

Group policy and per-user policy enforcement.

Group policy functions automatically create wireless profiles for your users. Whenever a new laptop user joins the domain, wireless access is available quickly.

You can also configure Active Directory for per-user policy enforcement. Supporting up to 64 policy configurations per an SSID, the system enables you to set up wireless access by user.

Also keep data secure by restricting guests to the Internet while allowing employees to connect to the Internet and your private network. You can even set it up so an authorized employee can create guest network accounts via the EMS.

Two options: Manage from a cloud or an appliance.

The **SmartPath EMS, Cloud-Based** version gives you either a 1-year (LWN600CM-1) or a 3-year subscription (LWN600CM-3) for managing one SmartPath AP. On-line management makes it easy to start small and add users to your network as you grow. And with no hardware device to install, configure, or patch, you can manage it from anywhere.

SmartPath on-line is hosted within secure Tier IV SAS 70 Type II data centers, with scheduled backups and disaster recovery capabilities and 24/7 monitoring. None of your traffic traverses the hosted service's network, so your data is kept private and secure.

For larger networks, you may prefer to use the **SmartPath EMS Appliance** (LWN600MA). It supports up to 2000 APs and is typically located within your facility. When using the appliance, you need to purchase a one-time perpetual license (LWN600MLA-1) for each AP.

SmartPath features in detail:

Wireless VPN capabilities

- An IPSec-based VPN solution for remote offices.
- Supports IPSec hardware acceleration.
- Profile-based split tunneling with NAT support.
- Wireless VPNs supported across mesh network.
- RADIUS, DHCP, NTLM, LDAP, and NTP can be selected to go to a local or remote network.

SLA compliance

- For health of client and APs, system monitors connection quality and triggers and reports on actions to improve quality.
- Automatically boosts, allocates airtime for clients to best reach performance targets.
- Balances loads for clients connecting to APs.

Security

- Wireless privacy and authentication is Wi-Fi CERTIFIED™, meeting WPA™ and WPA2™ protocols, and 802.11i, WEP, 802.1X, and PSK requirements.
- Granular user profile-based management defines VLANs, QoS, mobility policies, and security policies for each user entering the network.
- AES-CCMP, TKIP, and RC4 (WEP only) encryption.
- Mesh traffic encrypted with AES.
- Time-of-day and day-of-week access control and SSID enabling.
- Up to 16 SSIDs per radio for network segmentation.
- Onboard Stateful Inspection firewall policy enforcement with session state sync with neighbors.
- ALG support for SIP, DNS, TFTP, and FTP.
- Destination-based MAC firewall support.
- Tunnelled guest networks.
- Cluster-wide client isolation.
- WPA-TKIP vulnerability protection.

Authentication

- 802.1X authentication for WEP, WPA, and WPA2.
- Private PSK authentication enables unique preshared keys (PSK) for each user within a single SSID.
- RADIUS support with PEAP, EAP-TLS, TTLS, LEAP, and EAP-FAST.
- LDAP authentication to directory servers, including OpenLDAP®, Novell® eDirectory, and Apple® OpenDirectory®.

- Authentication to Microsoft® Active Directory™ with local credentials caching, also supports Global Catalog and multiple forests.
- Multiple RADIUS server support (per AP, per SSID).
- RADIUS server (local database or RADIUS proxy).
- Standard Interchange Protocol (SIP2) support for user validation vs. Library Information Systems (LIS).
- MAC-based RADIUS authentication.
- Dynamic Change of Authorization (RFC3576).
- 100 associated clients per LWN602HAE; 50 associated clients per LWN602AE.

Captive Web portal

- Built-in customizable captive Web portal on APs for guest access.
- Integrates easily with third-party Web portal solutions.
- RADIUS and Active Directory authentication support for the captive portal.

QoS for data, voice, and video at the radio

- Powerful QoS features, the kind typically only found on high-end routers.
- Supports Stateful VoIP roaming and failover.
- User profile-based queuing, scheduling, and policing.
- QoS can be assigned per VLAN, user profile, service, and MAC address.
- SIP call protocol decoding and dynamic port detection.
- Full queuing support with eight queues (strict and weighted round robin queuing mechanisms).
- Supports rate limiting per VLAN, per user profile, per user, and per service.
- VoIP call admission control (CAC).
- WMM® (802.11e) marking and policing for wireless, 802.1p, and/or DiffServ.
- Wi-Fi CERTIFIED WMM.
- WMM (U-APSD) power saving for Wi-Fi devices.
- Supports Spectralink® SVP wireless phone protocol.

Wireless IDS and IDP

- Built-in in-network rogue AP detection.
- Supports AirTight® IDS and IDP integration.
- Rogue AP mitigation and rogue client detection, including ad hoc clients.

- Wireless compliance checking.
- Sophisticated L2/L3 DoS protection with a wide range of L2/L3 attack signatures.
- Port scan, IP spoofing, and IP address sweep protection for added security, particularly for quarantine and guest networks.
- Wide array of security actions, including logging, blocking, disassociation, and banning, so the network can automatically respond to threats.

Mesh and availability

- Flexible radio configuration, enables either interface to be configured as a mesh.
- Ethernet bridging support across mesh connections for a single device or workgroup.
- Automatic neighbor detection and route determination in a mesh.
- Uses L2 routing instead of Spanning Tree for greater performance and less overhead.
- Self-healing enabled by dynamic path selection.
- For high availability, supports full client session synchronization across APs.
- Stateful failover of any AP, even in the event of a wired network failure.
- AAA caching of credentials for remote office survivability.
- Mesh failover in the event of wired network or switch failure. Automatically changes access radio to backhaul radio if such failure occurs.
- Wireless virtual access console.
- Track IP or gateway automatically initiates failover or troubleshooting tools in the event of a failure.
- Station (client) load balancing.
- Supports fast L2/L3 roaming and tunnel load balancing for L3 roaming.
- Wireless VPN supported across the mesh.

Redundant data support (LWN602HAE only)

- Dual Ethernet support for redundant data.
- Dual Ethernet connections enable link aggregation for legacy 10/100 or 10/100/1000 switches.
- Intelligently uses available power and adjusts as needs change.
- Enables you to benefit from 802.11n wireless while using legacy 10/100 or 10/100/1000 switches.

TECH SPECS

SmartPath APs:

Radio Frequencies — 802.11a: 5.150–5.950 GHz; 802.11b/g: 2.4–2.5 GHz; 802.11n: 2.4–2.5 GHz and 5.150 GHz–5.950 GHz
Radio Modulation — OFDM (802.11a/g), DSSS (802.11b), or 802.11n (802.11n)
Rated Speed — 300 Mbps
Operating Temperature — Indoor unit: +32 to +104° F (0 to +40° C); Hardened unit: -4 to +130° F (-20 to +55° C)
Connectors — Ethernet: (1) RJ-45 (indoor unit) or (2) RJ-45 (hardened unit), 10/100/1000 Mbps, PoE 802.3af and 802.3at compliant; Hardened unit only: Serial: (1) RJ-45 (RS-232)
Power — Either PoE or direct power; optional PoE Injector (LPJ001A-T) or 100–240-VAC, 50–60-Hz universal power supply (LWN600PS-EU) available
Size — Indoor unit: 2"H x 6.5"W x 6.5"D (5 x 16.5 x 16.5 cm); Hardened unit: 1.25"H x 8.5"W x 8"D (3.2 x 21.5 x 20.3 cm)
Weight — Indoor unit: 1.75 lb. (0.8 kg); Hardened unit: 3 lb. (1.4 kg)

SmartPath EMS Appliance:

Operating Temperature — +32 to +104° F (0 to +40° C)
Connectors — Wired LAN and management ports: (2) RJ-45 (10/100/1000 Mbps); Serial port: (1) DB9 M (RS-232); USB port: (1) USB Type A F (USB 2.0)
Power — Input: 100–240-VAC, 50–60-Hz, autoswitching, ATX, with PFC connector; Output: 250 watts
Size — 1.75"H (1U) x 16.8"W x 15.8"D (4.4 x 42.7 x 40.1 cm)
Weight — 13.75 lb. (6.2 kg)
SmartPath Outdoor Kit Enclosure Assembly
Protection Ratings — NEMA 4X, 6P (IEC IP56/IP67)
Wind Survivability — >265 km/h
Operating Temperature — -13 to +140° F (-25 to +60° C)
Connectors — For external antennas: (4) N-Type F
Size — 11.5"H x 14.25"W x 8.25"D (3.8 x 36.2 x 21 cm)
Weight — With hardened AP: 15 lb. (6.8 kg)

Why SmartPath Wireless?

Five top reasons to choose SmartPath:

1. It's designed for linear scalability.

Controller-less architecture eliminates unnecessary costs. 802.11n Wi-Fi becomes your primary access layer; you scale from small to large WLANs just by adding APs!

2. It's designed for high performance.

Features fully distributed, best-path data forwarding, and applies QoS and security at the APs while scaling network processing power linearly and reducing contention.

3. It's designed for reduced cost.

Unique architecture removes the need for controller hardware. Cloud-based management moves CAPEX to OPEX, enabling you to start small and grow as needed.

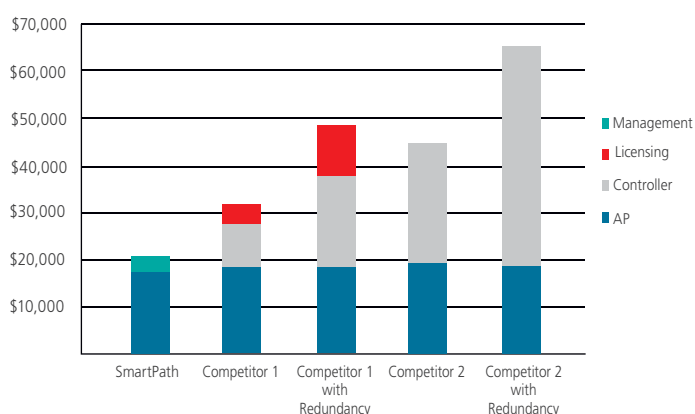
4. It's designed for ease of use.

Plug-and-play APs are paired with an easy-to-use Web interface featuring intuitive, policy-based management. This simplifies large deployments and gives you complete visibility of all network APs.

5. It's designed for high reliability.

Without a controller, there are no single points of failure or failover delays. "Smart," self-aware APs use dynamic mesh forwarding to create a path-resilient network.

Cost comparison: SmartPath vs. top competitors*:



The best thing about SmartPath Enterprise Wireless is its performance. But don't ignore its very low cost of entry. Versus its two leading industry competitors, it's very cost effective with no big investment to start and no waste as you grow. The main reason: SmartPath's unique architecture eliminates the need for an expensive controller. Plus, you can manage it from the cloud (or a local appliance). If management is lost, the APs will function normally—no backup controllers are needed for redundancy!

*(30) Indoor SmartPath APs (LWN602AE) managed via the cloud using (30) SmartPath Enterprise Management System 1-Year Subscriptions (LWN600CM-1) vs. competitor systems with (30) APs, management software, additional licenses (if required), controller(s), and support costs.
NOTE: SmartPath Cloud-Based EMS Subscriptions are represented above as "Management" expenses, and there is no separate license purchase required.

It's for you if you are:

- » Facing a forklift upgrade to move from 802.11a/b/g to 802.11n wireless.
- » Looking to economically deploy VoIP and real-time video over wireless.
- » An SME wanting to provide Internet access for employees and guests.
- » Tasked with providing universal Wi-Fi to new iPad® and smartphone users.
- » Dealing with CAPEX restrictions when trying to buy Wi-Fi equipment.

Item	Code
First choose your wireless AP(s)...	
SmartPath Wireless Access Point (AP)	
Indoor (with Integrated Antennas)	LWN602AE
Hardened (without Antennas)	LWN602HAE
...then select either a cloud-based management platform...	
SmartPath Enterprise Management System (EMS), Cloud-Based	
1-Year Subscription per AP	LWN600CM-1
3-Year Subscription per AP	LWN600CM-3
...or a standalone appliance with the required AP licenses ...	
SmartPath Enterprise Management System (EMS) Appliance (Up to 2000 APs)	LWN600MA
SmartPath Perpetual License for EMS Appliance (Perpetual, per Access Point)	LWN600MLA-1

Select the power option for your application:

802.3at PoE Gigabit Injector, 1-Port	LPJ001A-T
SmartPath 30-W Power Kit with Cord, Europe	LWN600PS-EU
For hardened APs, order...	
SmartPath 602HA Antenna Kit (Indoor Use)	LWN600A-ANTK
◆ Includes (3) 1.4 GHz and (3) 5-GHz antennas for (1) AP.	
SmartPath 602HA Outdoor Kit	LWN600A-OUT
◆ Includes (1) NEMA enclosure, (1) pole bracket, assorted hardware, (1) lightning protection device, (1) power supply, and (4) dual-band antennas for (1) AP.	

Click and find at blackbox.com/go/SmartPath.
US APs, plus US and U.K. power supplies.

© Copyright 2011. Black Box Corporation. All rights reserved. Printed in U.S.A. Black Box® and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Any third-party trademarks appearing in this publication are acknowledged to be the property of their respective owners.

LWN602AE-SmartPath_(27146)-priced_v1